Journal of Computer Applications
计算机应用,2013,33(8):2240 - 2243
ISSN 1001-9081
CODEN JYIIDU
2013-08-01
http://www.joca.cn

文章编号:1001-9081(2013)08-2240-04
doi:10.11772/j.issn.1001-9081.2013.08.2240

基于分层 Arnold 变换的置乱算法

张海涛[1],姚　雪[1*],陈虹宇[1],张　晔[2]
(1.辽宁工程技术大学 软件学院,辽宁 葫芦岛 125105;　2.哈尔滨工业大学 电子与信息工程学院,哈尔滨 150000)
(*通信作者电子邮箱 yaoyao5611@126.com)

摘　要:针对数字图像信息隐藏存在的安全问题,提出一种基于按位分层 Arnold 变换的置乱算法。算法将秘密图像按位平面分层,同时考虑图像的位置迁移和像素的灰度变换,对每个位平面进行不同次数的 Arnold 变换,经像素交叉换位,相邻像素间按位异或得出置乱图像。实验结果表明,秘密图像分层置乱后直方图分布更加均匀,与白噪声相似度在 0.962 左右,置乱图像可近无损地还原和提取,提高了信息隐藏的鲁棒性。与其他置乱算法相比,置乱图像具有更高的置乱度、更强的抵御攻击能力,提高了空域信息隐藏的安全性。

关键词:位平面;Arnold 变换;图像置乱;置乱度;空域信息隐藏
中图分类号:TP309.7　　**文献标志码**:A

Scrambling algorithm based on layered Arnold transform

ZHANG Haitao[1], YAO Xue[1*], CHEN Hongyu[1], ZHANG Ye[2]
(1. *College of Software, Liaoning Technical University, Huludao Liaoning* 125105, *China*;
2. *School of Electronics and Information Engineering, Harbin Institute of Technology, Harbin Heilongjiang* 150000, *China*)

Abstract: Concerning the safe problem of digital image information hiding, a scrambling algorithm based on bitwise layered Arnold transform was proposed. The secret image was stratified by bit-plane, taking into account the location and pixel gray transform, each bit-plane was scrambled for different times with Arnold transforma, and the pixel was cross transposed, and adjacent pixels were bitwise XOR to get a scrambling image. The experimental results show that the secret image histogram is more evenly distributed after stratification scrambling, its similarity with the white noise is around 0.962, and the scrambling image can be restored and extracted almost lossless, which improves the robustness. Compared with other scrambling algorithms, the proposed algorithm is more robust to resist attack, and improves the spatial information hiding security.

Key words: bit-plane; Arnold transform; image scrambling; scrambling degree; spatial information hiding

0　引言

数字图像置乱技术是图像加密的一种预处理方法,是进一步信息隐藏的基础工作。很多文献提出了可行有效的图像加密算法[1-3],算法的优劣直接影响图像的置乱度和图像信息隐藏的安全性。Fibonacci 变换[4]实质是错切变换、对称变换和切割回填;Hilbert 变换[5]实质是置乱路径和遍历图像;生命游戏变换[6]实质是对像素点以生命方式置乱,适者生存不适者灭亡;幻方变换实质是像素点的位置置乱;Arnold 变换实质是打乱图像相邻像素间的相互关联程度;相邻像素位异或置乱实质是通过像素位异或的方法扰乱图像灰度。其中 Fibonacci 变换、Hilbert 变换、生命游戏变换、幻方变换和 Arnold 变换仅仅是像素点位置的改变,灰度值并未发生变化[7]。

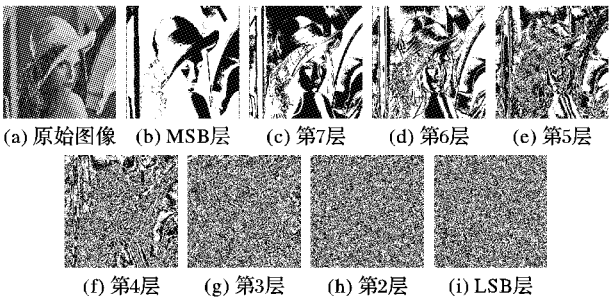
通过对经典图像置乱算法的分析和探讨,发现一些问题:算法只将图像像素点的位置变换,或只将灰度变化,考虑方面单一,置乱过程只考虑对原图分块或扫描为一维向量的形式,图像置乱的安全性低。针对以上问题,本文同时考虑图像像素点的位置和灰度变化,提出一种将图像按位进行分层置乱的算法,经实验可知,秘密图像置乱后灰度直方图(以下简称直方图)分布均匀,更接近于白噪声,与像素位置变换或图像灰度置乱算法相比,具有更高的置乱度。

1　图像分层理论

对灰度图像的置乱处理有很多,主要有全局置乱、分块置乱、单一像素值改变或置乱像素位置等方法[8]。本文提出分层的图像置乱算法,将图像按位平面分解为若干个二值图像,再作置乱处理。其基本原理为:依据灰度图像所具有的数据结构,设灰度图像为 $\boldsymbol{I}_{N\times N}$,灰度级为表示灰度取值范围所用二进制的位数,设灰度级为 0,1,2,…,$k-1$,则每一个二进制形式均可由灰度值 $a_0\cdot 2^0+a_1\cdot 2^1+\cdots+a_{k-1}\cdot 2^{k-1}$ 表示。256 级灰度图像的灰度级由 8 比特构成,所以将一幅秘密图像各像素点由高位到低位分割成 8 层,每个比特可以表示一个平面,即 8 个位平面,将其转化为 8 个独立的二值图像。其中:第一层由原图像各像素点二进制的最高位构成,形成最高位平面,记为 MSB;第二层由次高位构成;依此类推,形成 8 层二值图像。

选取 256×256 的 Lena 灰度图像,按位分解为 8 层,图 1 展示了从最高层至最底层分解得到的 8 层图像。

收稿日期:2013-03-05;**修回日期**:2013-04-18。　**基金项目**:国家自然科学基金资助项目(60972143)。
作者简介:张海涛(1974 -),男,黑龙江绥化人,副教授,博士研究生,CCF 会员,主要研究方向:图形图像处理、高光谱压缩;　姚雪(1988 -),女,辽宁朝阳人,硕士研究生,主要研究方向:图形图像处理;　陈虹宇(1989 -),男,辽宁朝阳人,硕士研究生,主要研究方向:图形图像处理、目标识别与跟踪;　张晔(1960 -),男,辽宁北镇人,教授,博士生导师,主要研究方向:图形图像处理、高光谱压缩。



(a) 原始图像　(b) MSB层　(c) 第7层　(d) 第6层　(e) 第5层

(f) 第4层　(g) 第3层　(h) 第2层　(i) LSB层

图 1　提取 8 层图像

2　Arnold 变换及其周期

Arnold 变换是 Arnold 在遍历理论研究中提出的一种变换,又称猫脸变换(cat mapping),是一种传统的混沌系统[9-10]。按相位空间可将 Arnold 变换分为二维、三维至 N 维变换,对于图像 $\boldsymbol{I}_{N\times N}$ 的二维 Arnold 变换矩阵形式如下:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \bmod N;\ (x,y) \in \{0,1,\cdots,N-1\} \tag{1}$$

其中:点 $(x,y)^{\mathrm{T}}$ 为原始坐标;$(x',y')^{\mathrm{T}}$ 为变换后坐标;N 为图像矩阵的阶。在不同阶数 N 下的 Arnold 变换周期性不同,当变换经过一定的迭代次数 T_N 后,将重新获得原始的水印图像[11]。对于 $N>2$ 的任意阶数,变换周期满足 $T_N \leqslant N^2/2$,如表 1 所列。

表 1　不同阶数 N 的变换周期 T

阶数 N	周期 T	阶数 N	周期 T	阶数 N	周期 T
4	3	90	60	180	60
8	6	100	85	190	90
16	12	110	30	200	150
32	24	128	96	210	120
40	30	130	210	220	30
60	60	140	120	230	120
64	48	150	300	240	60
70	120	160	120	250	750
80	60	170	90	256	192

随着迭代次数的增加,图像的置乱度逐渐升高,经文献[8]分析可得:当迭代次数大于 $T_N/2 \pm e$ 时($e \in \mathbf{N}_+$, $e \ll T_N$),图像的置乱程度开始降低,迭代 T_N 次回归到原始图像,据此,本文 3.1 节提出了适用于本文置乱算法的不同位平面置乱次数公式。

3　分层 Arnold 变换的置乱算法

本文算法的基本思想:首先对秘密图像按位分层,通过对每个位平面作不同次数的 Arnold 置乱变换、像素交叉换位、相邻像素间按位相异或,对图像进行加密,去除图像的自相关性,使置乱图像类似随机分布。

3.1　置乱步骤

步骤 1　读入数据。读取秘密图像。

步骤 2　图像分层。设原始秘密图像为 $\boldsymbol{A}_{M\times N}$,根据本文的图像分层理论,对原始图像 $\boldsymbol{A}$ 按位分层,形成 8 个位平面,记 $\boldsymbol{A}_i$ 为第 i 层,第一层 $\boldsymbol{A}_1 = \boldsymbol{A}_{\mathrm{LSB}}$,最高层 $\boldsymbol{A}_8 = \boldsymbol{A}_{\mathrm{MSB}}$。

步骤 3　各层置乱。在周期 T_N 内,从 $\boldsymbol{A}_{\mathrm{MSB}}$ 到 $\boldsymbol{A}_{\mathrm{LSB}}$ 层,对不同位平面 $\boldsymbol{A}_i$ 依次进行 C_i 次数 Arnold 置乱变换,置乱后记为 $\boldsymbol{A}_i'$。

$$C_i = \begin{cases} \dfrac{T_N}{2} \bmod M + (i-1)\left\lfloor \dfrac{T_N}{2M} \right\rfloor, & T_N \bmod 2M \neq 0 \\ e + (i-1)\left\lfloor \dfrac{T_N}{2M} \right\rfloor, & T_N \mid 2M \end{cases} \tag{2}$$

其中:T_N 为阶数 N 的周期;$i = 1,2,\cdots,8$;划分层数 $M = 8$,其置乱次数作为系统的密钥。

步骤 4　组合图像。组合各层置乱图像可视为图像分层的逆过程,即将置乱后的位平面 $\boldsymbol{A}_i'$ 按序重构为新的灰度图像,形成一张无色彩、无形状和无纹理的新图像 $\boldsymbol{S}$。

步骤 5　交叉换位。如图 2(bit1,bit2,…,bit8 分别表示每个像素点二进制灰度值的第 1,2,…,8 位),按从左到右、从上到下的顺序,将图像中的各个像素点 $S(m,n)$ 交叉换位,即:$b_1 \leftrightarrow b_8$;$b_2 \leftrightarrow b_7$;$b_3 \leftrightarrow b_6$;$b_4 \leftrightarrow b_5$,得到 $V(m,n)$。

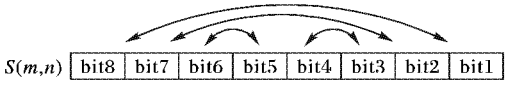
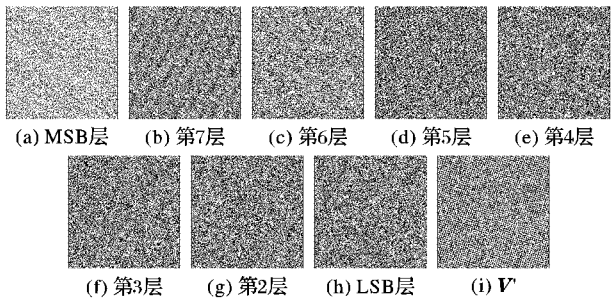


图 2　交叉换位示意图

步骤 6　异或运算。令第一个元素 $V(1,1)$ 与 255 相异或,得 $V'(1,1)$;令 $V'(1,1)$ 与 $V(1,2)$ 相异或,得 $V'(1,2)$;依此类推,$V'(m,n) \oplus V(m,n+1) \rightarrow V'(m,n+1)$,直到得到 $V'(M,N)$,则 $\boldsymbol{V}'$ 即是置乱后的秘密图像。

分层 Arnold 变换置乱算法举例:

图 1 展示了位平面由高到低的效果图,然后对各层图像做 C_i 次 Arnold 置乱变换,如图 3 所示,256×256 的 Lena 灰度图像变换周期 $T = 192$,取 $M = 8$,$e = 6$,则 $C_i = 6,18,30,\cdots,78,90$。各层置乱次数 C_i 作为密钥参数,增强了系统的安全性和保密性。各层图像组合后,经交叉换位和异或处理后最终得出置乱图像 $\boldsymbol{V}'$。



(a) MSB层　(b) 第7层　(c) 第6层　(d) 第5层　(e) 第4层

(f) 第3层　(g) 第2层　(h) LSB层　(i) $\boldsymbol{V}'$

图 3　各层图像置乱

3.2　逆置乱步骤

步骤 1　读取隐秘图像和密钥,密钥有秘密图像的尺寸类型和密钥参数等信息。

步骤 2　异或运算,$V'(m,n) \oplus V'(m,n-1) \rightarrow V(m,n)$,最后 $V'(1,1) \oplus 255 \rightarrow V(1,1)$,得到 $V(m,n)$。

步骤 3　对 $V(m,n)$ 进行交叉换位操作,操作如图 2 所示,换位后得到 $S(m,n)$。

步骤 4　将图像按位分解成 8 层,得到 8 张位平面图。

步骤 5　根据各层图像的置乱参数,对各层置乱图像 $\boldsymbol{A}_i'$ 进行不同次数的 Arnold 逆变换,得到 $\boldsymbol{A}_i$。

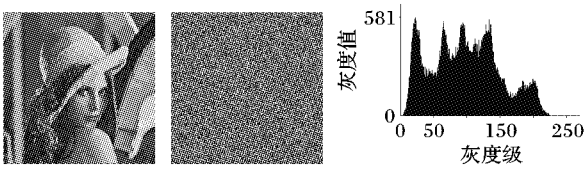
步骤 6　将得到的 8 个位平面 $\boldsymbol{A}_i$ 组合,得到原始秘密图像 $\boldsymbol{A}$。

4　实验结果与分析

基于上述算法,在 C#环境下进行仿真实验。

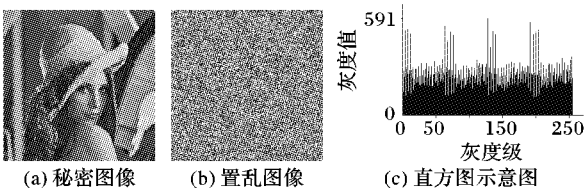
4.1 置乱比较实验

如图 4 ~6 所示,选取大小为 256 ×256 的 Lena 灰度图像作为秘密图像,运用三种方式对秘密图像置乱。Arnold 变换的置乱图像从人类视觉系统[15]的角度来说,无法看出图像的原始面貌,置乱后的直方图信息熵密集,置乱效果良好;文献[12]算法与 Arnold 变换相比,直方图发生明显变化,分布较匀;本文算法置乱图像纹理细腻,颗粒均匀,置乱最优,直方图分布均匀,趋于平缓,波动性小。



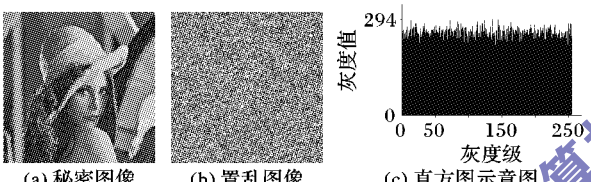
(a) 秘密图像 (b) 置乱图像 (c) 直方图示意图

图 4 Arnold 变换效果



(a) 秘密图像 (b) 置乱图像 (c) 直方图示意图

图 5 文献[12]算法效果



(a) 秘密图像 (b) 置乱图像 (c) 直方图示意图

图 6 本文算法效果

一幅图像的概貌信息分布可以通过其灰度直方图来描述,也可用直方图来分析图像的置乱效果。对于一幅类似白噪声的图像,其直方图均匀分布在整个区域,所以可以用与白噪声直方图的相似度来定量地衡量置乱效果,定义的相似度 α 如下:

$$\alpha = 1 - \frac{\sum_{k=0}^{G-1} |h_1(k) - h_2(k)|}{\sum_{k=0}^{G-1} |h_1(k) + h_2(k)|}; h(k) = n_k \tag{3}$$

其中:k 是指第 k 个灰度级,n_k 是灰度级的像素总和。纯噪声图像的直方图分布均匀,$h_1(i) = h_2(j)(i,j = 0,1,\cdots,G-1)$。根据式(3),不同算法置乱前后图像直方图与白噪声的相似度比较如表 2 所示。

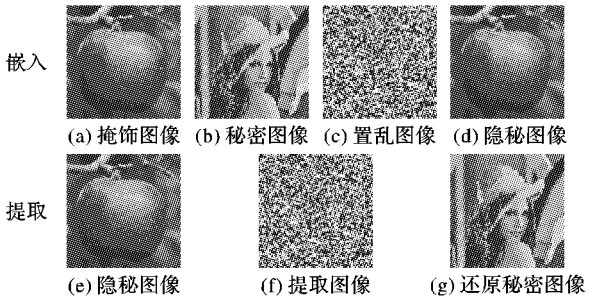
表 2 不同算法与白噪声直方图的相似度

图像	Arnold 变换	文献[12]算法	本文算法
原图像	0.621	0.621	0.621
置乱后图像	0.621	0.834	0.962

置乱比较实验表明,将通过本文算法生成的置乱图像应用在数字水印等信息加密隐藏的预处理中,图像的灰度直方图展开均匀,与白噪声相似度达到 0.962,置乱的图像信息可更加均匀地嵌入到掩饰图像中,得到的水印透明性更好,提高了信息的鲁棒性和安全性。

4.2 嵌入和提取实验

选取大小为 256 ×256 的 Apple 灰度图像作为掩饰图像(图 7(a)),选择文献[13]的嵌入算法,将 64 ×64 的 Lena 图像作为秘密图像(图 7(b)),按本文算法置乱形成置乱图像(图 7(c))后嵌入到图 7(a)中,形成隐秘图像(图 7(d));提取过程中,从图 7(d)中提取出图像(图 7(e)),最终按逆置乱方法还原秘密图像如图 7(f)。



(a) 掩饰图像 (b) 秘密图像 (c) 置乱图像 (d) 隐秘图像

(e) 隐秘图像 (f) 提取图像 (g) 还原秘密图像

图 7 图像的嵌入、提取结果

采用峰值信噪比(Peak Signal-to-Noise Ratio,PSNR)来衡量信息隐藏前后的相似度,保真度越好 *PSNR* 越大,定义如下:

$$PSNR = 10 \times \lg\left[\frac{M \times N \times 255^2}{\sum\sum (r_{ij} - r_{ij}')^2}\right] \tag{4}$$

其中:M、N 为载体图像的高和宽,r_{ij},r_{ij}' 为载体图像与融合图像(i,j) 位置对应的灰度值。

采用归一化相关系数(Normalized Correlation,NC)来评价提取的水印 W' 和原始水印 W 的相似性[14],W' 和 W 越相似 *NC* 值越大,定义如下:

$$NC = \frac{\sum\sum w_{ij} \otimes w_{ij}'}{m \times n} \tag{5}$$

其中:m、n 为水印图像的高和宽,w_{ij}、w_{ij}' 为嵌入和提取的水印图像 (i,j) 位置对应的灰度值,⊗为逻辑异或运算。

实验表明,本文置乱及逆置乱算法能有效地置乱和还原图像,对比实验选用不同的置乱算法分别嵌入图 7(a)中,分别计算其 *PSNR* 和 *NC* 值,结果如表 3 所列。本文置乱算法的峰值信噪比高于其他算法,归一化相关系数更接近于 1,可知隐秘图像在没有受到攻击的情况下,能够近无损地提取秘密图像。

表 3 嵌入不同置乱算法的 *PSNR* 和 *NC*

算法	*PSNR*/dB	*NC*
本文算法	45.010	0.999 98
Arnold 变换	42.098	1.000 00
文献[12]算法	43.042	0.999 84
文献[15]算法	44.010	0.999 87

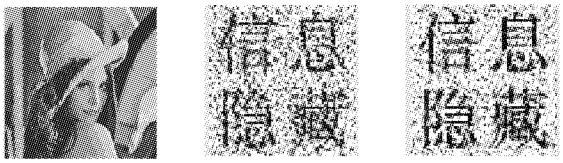
4.3 抗攻击实验

数字图像在传输过程中难免会受到噪声干扰等攻击,所以,置乱图像的抗攻击能力也是需要考虑的问题。实验将 64 ×64秘密图像嵌入到 256 ×256 的 Lena 掩饰图像中,对其进行椒盐噪声、中值滤波和剪切攻击实验。图 8 ~10 分别给出了含椒量 0.02 的椒盐噪声、窗口为[33]的中值滤波和左上剪切 1/4 的攻击提取效果图,以比较两种算法在加密后的图像受到相同攻击,再对其解密,解密图像与原图的相近情况;结果与原图越接近,该算法的抗攻击性能就越好。

表 4 列出了在不同攻击实验下,按照本文算法和文献[12]算法提取的图像的 *PSNR* 和 *NC*。实验结果表明,本文算法提取的秘密信息虽然夹杂着噪声,但秘密信息仍清晰可见,失真较少,且 *PSNR* 和 *NC* 值较大;随着攻击强度的降低,本文算法优于文献[12]的置乱算法。

(a) 隐秘图像(椒盐噪声0.02)　(b) 文献[12]算法的提取图像　(c) 本文算法的提取图像

图 8　椒盐噪声攻击、提取效果



(a) 隐秘图像(中值滤波[33])　(b) 文献[12]算法的提取图像　(c) 本文算法的提取图像

图 9　中值滤波攻击、提取效果

(a) 隐秘图像(左上剪切1/4)　(b) 文献[12]算法的提取图像　(c) 本文算法的提取图像

图 10　剪切攻击、提取效果

表 4　多种攻击实验比较结果

攻击方式	本文算法		文献[12]算法	
	PSNR/dB	*NC*	*PSNR*/dB	*NC*
椒盐噪声 0.1	18.203	0.9876	17.157	0.9589
椒盐噪声 0.02	24.718	0.9975	22.984	0.9752
均值滤波[55]	24.673	0.8532	20.930	0.7981
均值滤波[33]	27.496	0.8505	26.116	0.8134
左上剪切 1/4	14.826	0.9822	11.998	0.9682
中间剪切 1/4	10.582	0.9455	9.438	0.9283
左上剪切 1/8	17.017	0.9990	16.821	0.9743
中值滤波[55]	27.103	0.8992	23.454	0.8634
中值滤波[33]	29.915	0.8505	26.882	0.8429

4.4　置乱度比较

针对置乱图像与原始图像对应位置像素值偏离的程度,文献[16]提出基于信噪比(Signal-to-Noise Ratio,SNR)的数字图像置乱程度评价方法,将原始数据与重现图像数据之差看作“噪声”。设 $N\times N$ 个原始数据由 $f(x,y)(x,y\in\{0,1,\cdots,N-1\})$ 表示,重现的图像数据表示为 $g(x,y)(x,y\in\{0,1,\cdots,N-1\})$,此时噪声为 $e(x,y)=f(x,y)-g(x,y)$。重现图像的均方信噪比定义为:

$$(SNR)_{ms}=\frac{\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}g^2(x,y)}{\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}e^2(x,y)} \tag{6}$$

图像置乱度定义为式(7),t 为图像分成的块数:

$$\eta=1/s;\ s=\sum_{i=1}^{t}SNR_i/t \tag{7}$$

从表 5 可以看出,使用基于图像高亮度的信噪比(SNR)的数字图像置乱度评价方法来衡量图像的置乱度,与仿射变换、Arnold 变换和文献[12]置乱算法比较而言,本文算法的置乱度明显高于其他方法,即用本文算法置乱的图像相对于原始图像偏离程度更大,置乱效果更好。

表 5　不同算法置乱图像与原图像的置乱度

算法	置乱度
仿射变换	0.1223
Arnold 变换	0.1000
文献[12]算法	0.3621
本文算法	0.6218

5　结语

本文针对现有图像置乱算法存在的缺点,提出了基于分层 Arnold 变换的置乱算法,并进行了仿真对比实验。实验结果表明,本文算法置乱图像纹理细腻,直方图分布均匀,置乱特征接近白噪声,相似度能达到 0.962,得到的水印透明性更好,提高了信息隐藏的安全性;算法能近无损地提取图像,PSNR 值均大于其他算法,满足了无失性;在椒盐噪声、中值滤波、剪切攻击和均值滤波攻击方面优于其他算法,具有良好的抗攻击能力,更加适用于加密传输。

参考文献:

[1] JOLFAEI A, MIRGHADRI A. Image encryption using chaos and block cipher[J]. Computer and Information Science, 2011, 4(1): 172 – 185.

[2] NAYAK C K, ACHARYA A K, DAS S. Image encryption using an enhanced block based transformation algorithm [J]. International Journal of Research and Review in Computer Science, 2011, 2(2): 275 – 279.

[3] 贺楚雄, 田绍槐. 基于灰度级出现频数的数字图像置乱程度衡量方法[J]. 中国图象图形学报, 2010, 15(2): 220 – 228.

[4] 邹建成, 石志鑫. 一种基于 Fibonacci 数系的数字水印新方法[J]. 电子学报, 2011, 39(7): 1598 – 1602.

[5] 张荣祥, 郑世杰, 夏庆观. 基于 Hilbert 扫描和小波变换的自适应图像分割[J]. 中国图象图形学报, 2008, 13(4): 666 – 671.

[6] 郭娟, 吴迪, 赵宪明. 生命游戏复杂性的模拟研究[J]. 计算机仿真, 2007, 24(10): 285 – 289.

[7] 蔡邦荣. 数字图像置乱评估方法研究[D]. 大连: 大连理工大学, 2011.

[8] KADIR R, SHAHRIL R, MAAROF M A. A modified image encryption scheme based on 2D chaotic map [C]// Proceedings of 2010 International Conference on Computer and Communication Engineering. Piscataway: IEEE, 2010: 1 – 5.

[9] 黄良永, 肖德贵. 二值图像 Arnold 变换的最佳置乱度[J]. 计算机应用, 2009, 29(2): 474 – 476, 483.

[10] NINASSI A, le MEUR O, le CALLET P, *et al*. On the performance of human visual system based image quality assessment metric using wavelet domain [C]// HVEI 2008: Human Vision and Electronic Imaging XIII, SPIE 6806. Bellingham: SPIE, 2008: 680610.

[11] RIAD A M, HUSSEIN A H, KASEM H M, *et al*. A new efficient image encryption technique based on Arnold and IDEA algorithms [C]// ICIIP 2012: Proceedings of the 2012 International Conference on Image and Information Processing, IPCSIT 46. Singapore: IACSIT Press, 2012: 140 – 145.

[12] 何冰. 基于仿射变换的图像置乱改进新算法[J]. 计算机与数字工程, 2011, 39(3): 121 – 124.

[13] 王颖慧, 刘万军. 基于 MSB 和 HVS 的空域信息隐藏算法的研究[J]. 计算机科学, 2012, 39(9): 89 – 93.

[14] 李峰, 陈光喜, 丁勇, 等. 基于混沌和 HVS 的小波域自适应图像水印算法[J]. 计算机应用研究, 2012, 29(6): 2224 – 2227.

[15] 刘挺. 一种基于 HVS 的空域分块数字水印技术[J]. 电子设计工程, 2012, 20(6): 184 – 185, 189.

[16] 李志伟, 陈燕梅, 张胜元. 基于 SNR 的数字图像置乱程度评价方法[J]. 厦门大学学报: 自然科学版, 2006, 45(4): 484 – 487.